"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology

A. MICHAEL FROOMKIN*

TABLE OF CONTENTS

I. INTRODUCTION

With the exception of a relatively small number of relationships defined by statute or custom,[1] privacy[2] is not mandated by default in the United States.[3]

---

* Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law, University of Miami. This paper was inspired by Claudia Diaz's presentation on European law's conflicts with PETs, *Hero or Villain: The Data Controller in Privacy Law and Technology*, delivered at the *Ohio State Law Journal*'s symposium on "The Second Wave of Global Privacy Protection." *See* Claudia Diaz, Omer Tene & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923 (2013). I would like to thank Peter Swire and the editors of the *Ohio State Law Journal* for allowing me to substitute this different—and more timely—essay for the one I presented at the conference. Also, thanks to Irakli Shalolashvili for research assistance, and to Caroline Bradley, Peter Eckersly, and Lee Tien for helpful conversations. Unless otherwise noted, this article seeks to reflect technical and legal developments up to Aug. 28, 2013. The update in Part V seeks to reflect news reports up to Sept. 21, 2013.

[1] E.g., attorney–client privilege. *See* MODEL CODE OF PROF'L RESPONSIBILITY Canon 4 (1978); MODEL RULES OF PROF'L CONDUCT R. 1.6 (2013).

[2] For the purposes of this Article, I define privacy to mean informational privacy, and more specifically the ability to control the release of information about oneself. This

Thus, in almost all legal and social relationships, and in most of daily life, if one wishes to keep something private as a legal matter, each of us in the United States bears the responsibility to arrange our own affairs so that we achieve our privacy goals. That state of affairs is itself no secret; it is regularly publicized, and most people must by now be aware that if they care about their privacy they must protect it. What is less well understood, however, is the extent to which the law—and commercial practice also—actually imposes impediments to privacy. This Article examines some of those impediments, particularly legal rules and corporate policies that block (or seem likely in the near future to be invoked to block) privacy self-help in the form of Privacy Enhancing Technologies (PETs) and other privacy enhancing measures.[4]

PETs and other privacy enhancing measures are important because of increasing private sector surveillance online and in daily life. Privacy enhancement also seems particularly important now in light of recent revelations regarding the United States government's systematic collection of communications meta-data, and of at least some actual communications data.[5] Corporate policies matter because in industries subject to concentration—whether due to ordinary oligopoly or the network effects that frequently characterize communications technologies—these private rules constrain consumer choices much as do the legal rules. What is more, the two converge: industry concentration provides an easy locus for regulation; alternately, the threat of regulation can drive an industry to adopt rules and practices favoring a government agenda.[6] A government concerned with protecting personal privacy and enhancing user security against ID theft and other fraud should support and advocate for the widespread use of PETs. In fact, however, whatever official

---

definition is admittedly incomplete, but it has a pedigree, see e.g., ALAN F. WESTIN, PRIVACY AND FREEDOM 7–12 (1967), and this is a short Article.

[3] For a thoughtful discussion of why privacy by default makes sense, and the likely consequences of making it the default, see Lauren E. Willis, Why Not Privacy by Default? (Aug. 2013) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349766 (on file with author).

[4] A standard definition of PETs is in G.W. VAN BLARKOM, J.J. BORKING & J.G.E. OLK, HANDBOOK OF PRIVACY AND PRIVACY-ENHANCING TECHNOLOGIES: THE CASE OF INTELLIGENT SOFTWARE AGENTS 33 (2003), *available at* http://www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf.

[5] *See infra* text following note 50.

[6] *See infra* text at notes 84–87 (discussing motivations for adoption of Trusted Computing by chip makers); *see also* Declan McCullagh, *How the U.S. Forces Net Firms To Cooperate on Surveillance*, CNET NEWS (July 12, 2013, 12:30 PM), http://news.cnet.com/8301-13578_3-57593538-38/how-the-u.s-forces-net-firms-to-cooperate-on-surveillance/ (firms threatened with surveillance orders in order to secure "voluntary" compliance with U.S. surveillance demands); Tom Simonite, *Microsoft's Surveillance Collaboration: Voluntary Aid, or New Legal Tactic?*, MIT TECH. REV. (July 12, 2013), http://www.technologyreview.com/news/517151/microsofts-surveillance-collaboration-voluntary-aid-or-new-legal-tactic/ (speculating as to motives for Microsoft's redesign of Outlook.com email service in order to enable National Security Agency's PRISM surveillance program to collect chat data before it was encrypted).

policy may be, by its actions the prevailing attitude of the U.S. government amounts to saying that PETs, and indeed other privacy protecting technology, must be kept on a leash.

II. WHY CONSUMERS NEED PETS AND OTHER PRIVACY DEFENSES

During an average day most of us do things in the home. We move around outside the home. We make phone calls on landlines or cell phones. Many of us use the Internet to read or write, either on computers or, increasingly, on hand-held devices. We engage in transactions online, in stores, or with service providers such as doctors and lawyers. Each of these activities has varying elements of privacy; increasingly, however, whether we want them to or not, each of these activities generates extensive records available to different private and public entities.

Maintaining one's privacy limits the extent to which others can use these types of personal information—legally—to exercise various sorts of power against one. The more that other people know, the more they may make invidious judgments, practice price discrimination, target advertising, or engage in other legal acts that one might prefer to avoid.[7] Privacy also protects against some illegal activities such as credit card fraud and identity theft.[8] For some, privacy may also be a good in itself.

Both the U.S. government and the U.S. national media have made it clear that, in the main, privacy protection is a personal responsibility. Thus, for example, the U.S. Department of Justice, Bureau of Justice Assurance has funded an illustrated guide for consumers on "Preventing Identity Theft,"[9] which instructs consumers to avoid putting outgoing mail, especially bill payments, in private mailboxes where it can be stolen, not to write account numbers where they can be seen, to "[m]ake sure nobody is standing right

---

[7] *See, e.g.*, Ryan Calo, *Digital Market Manipulation* 31–34 (Univ. of Wash. Sch. of Law Legal Studies, Research Paper No. 2013-27, 2013), *available at* papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703 (discussing likely harms consumers may suffer when profiled by marketers and other corporations).

[8] Identity theft—defined in these sources as including credit card fraud, which is actually a less serious fraud than the assumption of an identity for other purposes also—is on the rise. *See* Kate Rogers, *One New Identity Theft Victim Every 3 Seconds in 2012*, FOXBUSINESS (Feb. 20, 2013), http://www.foxbusiness.com/personal-finance/2013/02/20/one-new-identity-theft-victim-every-3-seconds-in-2012/; Bob Sullivan, *ID Theft on the Rise Again: 12.6 Million Victims in 2012, Study Shows*, NBCNEWS (Feb. 20, 2013, 12:00 AM), http://redtape.nbcnews.com/_news/2013/02/20/17022584-id-theft-on-the-rise-again-126-million-victims-in-2012-study-shows?lite; Martha C. White, *Study: 10,000 Identity Theft Rings in U.S.*, TIME, Nov. 20, 2012, http://business.time.com/2012/11/20/study-10000-identity-theft-rings-in-u-s/.

[9] *See* NAT'L CRIME PREVENTION COUNCIL, PREVENTING IDENTITY THEFT: A GUIDE FOR CONSUMERS (July 2005), *available at* http://www.ncpc.org/cms-upload/prevent/files/IDtheftrev.pdf. The illustrations feature McGruff, the Crime Dog. The Justice Department's funding is acknowledged on the copyright page.

behind you when you're using an ATM", and not to "give out your credit card number on the Internet unless it is encrypted on a secure site."[10] Other helpful suggestions include "examine your credit reports," "make sure no one is listening" if giving out personal information on a cell phone in a public place, "[s]hred all financial statements," "[m]inimize the number of identification and credit cards you carry with you," "[u]se traveler's checks instead of personal bank checks,"[11] "be alert," "[c]ommit all passwords to memory. Never write them down," and "[g]ive out your Social Security number only when absolutely necessary."[12] A similar focus on self-defense characterizes other consumer-oriented government publications, such as the FDIC's video, *Don't Be an On-Line Victim: How To Guard Against Internet Thieves and Electronic Scams*.[13] Official policy of some agencies, however, can be more nuanced, as can be seen for example in the FTC's recent report on the use of Social Security Numbers (SSNs).[14] In contrast to the consumer-facing publications, the report suggests a number of measures to reduce commercial requests for SSNs—and also more consumer education in self-help.[15]

Similarly, both print and online media are replete with advice as to how consumers should protect their privacy. Some of it is reasonably sophisticated. For example, Forbes.com's *10 Incredibly Simple Things You Should Be Doing To Protect Your Privacy* advises using a proxy service such as Tor to mask IP numbers when visiting web sites.[16]

In fact, however, the average person who wishes to preserve his or her privacy has only a limited variety of actions available to choose from in order to achieve any privacy objectives: alter one's daily behavior, contract for additional privacy, or employ technological defenses. Each of these strategies faces serious limitations, both practical and legal.

---

[10] *Id.* at 7.

[11] *Id.* at 8. Oddly the National Crime Prevention Council does not discuss the extra fees required to purchase travelers checks, the float buying travelers checks gives banks (and the lost interest it would cause consumers), nor the increasing unwillingness of merchants to accept travelers checks as they become less and less common. *See, e.g.*, Kerri Fivecoat-Campbell, *Death of the Traveler's Check*, MSN MONEY (Mar. 8, 2011, 6:06 PM), http://money.msn.com/saving-money-tips/post.aspx?post=6e420c77-ad08-4549-ae08-7aa58800d3ea.

[12] PREVENTING IDENTITY THEFT: A GUIDE FOR CONSUMERS, *supra* note 9, at 9.

[13] *Don't Be an On-Line Victim: How To Guard Against Internet Thieves and Electronic Scams*, FDIC, http://www.fdic.gov/consumers/consumer/guard/index.html (last updated June 22, 2011); *see also* SOC. SEC. ADMIN., SOCIAL SECURITY: IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER 2–4 (Oct. 2012), *available at* http://www.socialsecurity.gov/pubs/EN-05-10064.pdf; SOC. SEC. ADMIN., SOCIAL SECURITY: YOUR SOCIAL SECURITY NUMBER AND CARD 11–12 (Aug. 2012), *available at* http://www.ssa.gov/pubs/EN-05-10002.pdf.

[14] FED. TRADE COMM'N, SECURITY IN NUMBERS: SSNS AND ID THEFT 2–3 (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf.

[15] *See id.* at 10 ("Conduct Outreach to Business and Consumers").

[16] Kashmir Hill, *10 Incredibly Simple Things You Should Be Doing To Protect Your Privacy*, FORBES (Aug. 23, 2012), http://www.forbes.com/sites/kashmirhill/2012/08/23/10-incredibly-simple-things-you-should-be-doing-to-protect-your-privacy/.

A. *Limits to Changing Daily Behavior*

One's daily behavior has very great privacy consequences, only some of which are under a person's control. For example, one can choose whether to patronize businesses with CCTV cameras, whether or not to be on Facebook, and what to post online if one chooses to be on Facebook. One can wrestle with Facebook's ever-changing privacy settings. But any person living in a modern industrialized country will find that there is only so much that even living in a very privacy-conscious fashion can do. Cameras are often cleverly camouflaged, and they are increasingly prevalent.[17] Whether or not one chooses to be on Facebook, one cannot control what pictures other people might put on Facebook and how they identify or tag them.

Short of hiding out in a cabin in the woods—with sufficiently dense year-round foliage to foil overflights, drones, and satellites—or perhaps hiding behind an ever-changing series of disguises, regularly changing pre-paid cell phones and numbers, and paying for everything in cash, the tracked, surveilled, examined, and analyzed life is now pretty much an unavoidable aspect of urban and even rural life. Even in normal, non-hermetic life, the law imposes some constraints on privacy. Increasingly one is required to identify oneself to use mass transit—first airplanes, and now trains and perhaps buses.[18] Searches to enter federal buildings are now routine;[19] random searches in other public places are increasingly commonplace.[20] "Postal Service computers photograph the exterior of every piece of paper mail that is processed in the United States — about 160 billion pieces last year."[21] And, ever since the *Hiibel* decision,[22] states have had the power to compel anyone being investigated by the police to identify themselves. Meanwhile, the private sector is increasingly deploying

---

[17] For a cautionary tale based on the UK experience see Benjamin Goold, Ian Loader & Angélica Thumala, *The Banality of Security: The Curious Case of Surveillance Cameras*, 53 BRIT. J. CRIMINOLOGY 977 (2013), *available at* http://bjc.oxfordjournals.org/content/early/2013/07/22/bjc.azt044.full.pdf+html (noting both pervasiveness of CCTV in the UK and the resulting desensitization of the public—or as they call it, the growing "banality" of CCTV).

[18] *See Passenger Identification*, AMTRAK, http://www.amtrak.com/passenger-identification (last visited Nov. 8, 2013); *Is an ID Required To Travel by Bus?*, PETER PAN BUS LINES (June 13, 2013, 3:43 PM), support.peterpanbus.com/entries/21699644-Is-an-ID-required-to-travel-by-bus-; *see also* Yofi Tirosh & Michael Birnhack, *Naked in Front of the Machine: Does Airport Scanning Violate Privacy?*, 74 OHIO ST. L.J. 1263 (2013).

[19] *See* Declan McCullagh & Anne Broache, *Federal Buildings Become Real ID Zones*, CNET NEWS (Feb. 5, 2008), http://news.cnet.com/Federal-buildings-become-real-id-zones/2009-1028_3-6229133.html.

[20] *See* MacWade v. Kelly, 460 F.3d 260, 269, 275 (2d Cir. 2006) (holding that random bag searches on N.Y.C. subway were reasonable).

[21] Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y. TIMES, July 3, 2013, http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?smid=pl-share.

[22] Hiibel v. Sixth Judicial Dist. Court of Nev., 542 U.S. 177, 190–91 (2004).

cameras to monitor the public, both as security cameras on private property[23] and as part of mass tracking designed to feed "smart city" initiatives.

B. *Limits to Contracting for Privacy*

One major form of lost privacy comes in the form of the digital records left by economic transactions. In theory, one ought to be able to contract with firms for increased privacy. In practice, of course, most goods and services are provided on mass-market terms in which the supplier provides a non-negotiable standard form contract.[24] The idea that in any but a negligible fraction of cases one would be able to alter those terms by negotiation is laughable.

One might expect, however, that if there is a demand for privacy, then in a capitalist economy firms would seek to differentiate themselves by competing on privacy. And indeed, there are a small number of primarily online services that market themselves as privacy-friendly. Thus, for example, DuckDuckGo and Ixquick market themselves as privacy-friendly search engines. Indeed, as I write this, Ixquick's home page calls itself "the world's most private search engine."[25] Every search result has a small hyperlinked announcement running at the top which reads "Giant US government Internet spying scandal revealed."[26] Ixquick returns the top ten results from multiple search engines and asserts that it does not store any user data and that it uses https encryption by default.[27] It also boasts that because Ixquick is based in the Netherlands,

> US jurisdiction does not apply to us, at least not directly. Any request or demand from ANY government (including the US) to deliver user data, will be thoroughly checked by our lawyers, and we will not comply unless the law which actually applies to us would undeniably require it from us. And even in that hypothetical situation, we refer to our first point; we don't even have any user data to give. We will never cooperate with voluntary spying programs like PRISM.[28]

With these promises Ixquick attempts to distinguish itself from the larger and more popular search engines, and especially from Google, the market

---

[23] The spread of security cameras (aka CCTV) is an international phenomenon. *See generally Revisiting the Surveillance Camera Revolution: Issues of Governance and Public Policy. Introduction to Part One of the Special Issue*, 16 INFO. POLITY 297 (2011). Surveillance in the United States is taking on a new, more intrusive, dimension with the deployment of "smart city" and "urban informatics" initiatives. *See, e.g.*, Steven E. Koonin, Dir., Ctr. for Urban Sci. and Progress, *The Promise of Urban Informatics* (Aug. 2, 2013).

[24] *See* MARGARET JANE RADIN, BOILERPLATE 82–98 (2013).

[25] *See* IXQUICK, https://ixquick.com (last visited Sept. 10, 2013).

[26] *See No PRISM. No Surveillance. No Government Back Doors. You Have Our Word on It*, START PAGE, https://startpage.com/eng/prism-program-exposed.html (last visited June 27, 2013).

[27] *Id.*

[28] *Id.*

leader. Interestingly, for those seeking fuller search results, Ixquick offers a service called Startpage in which it acts as an anonymizing intermediary between the user and Google.[29] Note, however, that if the government has direct access to Internet Service Providers (ISPs) and cell phone companies, it can acquire copies of all search requests before they get to Ixquick or any other search engine. Only if those requests are encrypted at the source, e.g. via SSL or TLS, will the use of a foreign-based search engine provide much in the way of security against dragnet wiretaps. And even then, that security is only as good as the search engine provider's protection of its encryption keys.[30]

The search engine market is, unfortunately, atypical: it is relatively easy to run an Internet search provider from off-shore as the product is entirely virtual, and the search engine industry is not heavily regulated (as compared to banks for example). These conditions are not unique to search engines, but they are true of only a subset of primarily Internet-related service industries, or industries dealing in intangibles or in digitizable property.[31] They do not apply to economic transactions that involve the exchange of a physical good, or an in-person service, or require the participation of a firm in a heavily regulated industry. Nor does the competition argument work well in industries subject to network effects[32] or to any other economic forces that encourage concentration.

Regulation also plays a part in suppressing competition on privacy. United States-based participants in heavily regulated industries such as banks and securities trading could not offer substantially privacy-enhanced terms of service even if they wished to; they have some small amount of flexibility on the extent to which they share customer information with affiliated companies or third parties,[33] but that is about it.[34] Significant competition on privacy is not possible because U.S. law imposes strict anti-privacy requirements on financial

---

[29] *See Privacy*, START PAGE, https://www.startpage.com/eng/protect-privacy (last visited Sept. 10, 2013).

[30] *See* Brett Wooldridge, *Duck Duck Go: Illusion of Privacy*, ETHER RAG (July 11, 2013), http://etherrag.blogspot.com/2013/07/duck-duck-go-illusion-of-privacy.html. Note that several—but not all—of the critiques in this article only apply to U.S.-based search engines.

[31] *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129, 129–54 (Brian Kahin & Charles Nesson eds., 1997) (predicting, so far accurately, that "most regulation of tangible goods . . . will remain unaffected by the Internet").

[32] On network effects and competition, see Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP., Spring 1994, at 93, 93; Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1682–84 (2013).

[33] *See* M. MAUREEN MURPHY, CONG. RESEARCH SERV., RS20185, PRIVACY PROTECTION FOR CUSTOMER FINANCIAL INFORMATION 1–3 (2012), *available at* http://www.fas.org/sgp/crs/misc/RS20185.pdf.

[34] *See Fact Sheet 24: Protecting Financial Privacy: The Burden Is on You*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/content/protecting-financial-privacy-burden-you (last visited Nov. 11, 2013).

services providers. Banks and brokers must "know their customers"[35] and must report all transactions exceeding $10,000 to the federal government; some money-moving entities must report transactions exceeding $2,500.[36]

Other rules sweep more broadly. For example the "third-party doctrine" means that as soon as Alice allows another to know information about her—including intermediaries such as her cell phone company or her bank—she has effectively waived her Fourth Amendment rights to that information.[37] In *United States v. Jones*, Justice Sotomayor questioned the continuing validity of the third-party doctrine, suggesting that:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.[38]

Justice Sotomayor's concerns are well-taken, but pending any reform of the third-party doctrine, the fact remains that anyone sending an unencrypted email is in effect at the mercy of every intermediary in the possibly lengthy chain of intermediaries if the government comes calling with a warrant—or even, it seems, if it comes without one.[39] A number of laws, for example the Electronic

---

[35] Bank Records and Foreign Transactions Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970).

[36] *See* Genci Bilali, *Know Your Customer—or Not*, 43 U. TOL. L. REV. 319, 320–21 (2012) (surveying relevant laws and rules); Rosalie Rayburn, *Suspicious-Transaction Reporting Alarms Privacy Advocates*, ALBUQUERQUE J., Apr. 11, 2004, http://www.abqjournal.com/biz/160454business04-11-04.htm (relating to transactions over $2,500); *see also* Ross Q. Panko, *Banking on the USA PATRIOT Act: An Endorsement of the Act's Use of Banks To Combat Terrorist Financing and a Response to Its Critics*, 122 BANKING L.J. 99, 99–102 (2005) (endorsing requirements that banks share customer information with both law enforcement and other banks if the person is suspected of illegal activity).

[37] Perhaps the strongest defense of the third-party doctrine is Orin S. Kerr's *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561–65 (2009). Kerr argues that the third-party doctrine ensures the technological neutrality of the Fourth Amendment. Without it, criminals could substitute a hidden third-party exchange for a previously public act. Kerr also argues that the rule's (to me, Procrustean) simplicity is an important virtue. *Id.* at 563.

[38] Unites States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

[39] That the United States' National Security Agency (NSA) has systematically been capturing all or part of communications by millions of U.S. citizens and others has been known since at least 2001. *See* Jewel v. NSA, Order on Motions for Summary Judgment (N.D. Cal. July 8, 2013) (rejecting state secrets defense relating to alleged illegal NSA

Communications Privacy Act,[40] protect against communications intermediaries snooping on private communications. Not everyone is law-abiding, however, and as a result a privacy- and safety-conscious person needs to protect herself against those intermediaries as best she can.

The privacy problem is every bit as great in the private sector. Whereas in the '90s it might have been easy to argue that market forces would sort out the privacy and anti-privacy policies of firms, leading firms to compete to be seen as privacy-friendly or to position themselves along a spectrum of privacy by offering policies that would distinguish them from their competitors, that argument seems less plausible today for reasons that have little to do with privacy itself. The past decade has witnessed a powerful market-driven shift towards closure and centralization in both hardware (e.g. the iPhone) and software (e.g. Facebook, Twitter).

Facebook is a leading example of this phenomenon. It is wildly popular, and, at least for a time, seemed poised to become the center of a constellation of applications that link to or from it, or rely on credentials that Facebook provides.[41] For most of its existence, however, Facebook has pursued policies that require users to identify themselves uniquely.[42] Facebook is dominant in

---

spying and permitting case to go forward on constitutional claims), *available at* https://www.eff.org/node/74895; *NSA Spying on Americans*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/nsa-spying (describing discovery of AT&T cooperation with illegal NSA surveillance). As this is being written, revelations continue to emerge about the alleged, and at times admitted, program of warrantless wiretapping by the NSA. *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008) (approving order requiring telecommunications service provider to assist in warrantless surveillance of persons "reasonably believed" to be outside United States); James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, GUARDIAN, Aug. 9, 2013, http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (warrantless acquisition of communications of U.S. persons). For an early discussion of some of the legal issues see Blake Covington Norvell, *The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation?*, 11 YALE J.L. & TECH. 228 (2009).

[40] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510–2522).

[41] Caroline McCarthy, *Amid Unrest, a Hard New Look at Online Anonymity*, CNET (Feb. 22, 2011, 3:33 PM), http://news.cnet.com/8301-13577_3-20034879-36.html; *see also* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1146 (2009) ("Facebook's most technologically interesting feature is its 'Platform,' which developers can use to create 'Applications' that plug seamlessly into the Facebook site."). *But see* Hamish McKenzie, *Move Fast, Break Things: The Sad Story of Platform, Facebook's Gigantic Missed Opportunity*, PANDODAILY.COM (July 23, 2013), http://pandodaily.com/2013/07/23/move-fast-break-things-the-sad-story-of-platform-facebooks-gigantic-missed-opportunity/ (arguing that Facebook failed to exploit potential of its Platform and thus allowed Apple iOS and Google's Android to become the dominant platforms for apps).

[42] *Data Use Policy: Information We Receive About You*, FACEBOOK, https://www.facebook.com/about/privacy/your-info (last visited Nov. 9, 2013) ("When you sign up for

size, but by no means unique: many other social networks also require users to use their real names. Google+, a recent entrant to social networking, requires participants to "use the name your friends, family, or co-workers usually call you," or "the name that you commonly go by in daily life"—a policy that has been subject to substantial criticism.[43]

Firms, Google chief among them, seek to monetize user-generated content in a variety of ways that often (although not inevitably) require the identification of the user at least with a persistent token such as a cookie or something similar,[44] if not their actual name. Thus, for example, business models that rely on serving targeted advertising need to know relevant facts about the target's tastes and habits, and also may want to know what ads have already been seen in order to avoid repetition. A "persistent token" may sound innocuous, but if any application that uses the token links to the user's real identity, or even in some cases his geo-location, the token becomes an effective identification technology. Similar risks apply to users of many current cloud-based services.[45]

In each of these cases, leading firms in their industry have chosen to require user self-identification as the price of access to their highly desirable network. No government regulation was involved. We have known for some time that the U.S. government was well aware that banks and other financial service providers, ISPs, telecommunications providers and other key market participants, were effective chokepoints for transactions flows and communications. Indeed the U.S. government relies on these chokepoints as targets for regulation aimed at end-users. With recent revelations about the NSA, we are only now learning that the U.S. government also used these same

---

Facebook, you are required to provide information such as your name, email address, birthday, and gender.").

[43] *See* Identity Woman (Kaliya Hamlin), *Google+ and My "Real" Name: Yes, I'm Identity Woman*, IDENTITYWOMAN.NET (July 31, 2011), http://www.identitywoman.net/googlereal-name-identity-woman; *see also* Kee Hinckley, *On Pseudonymity, Privacy and Responsibility on Google+*, GOOGLE PLUS (July 27, 2011), https://plus.google.com/117903011098040166012/posts/asuDWWmaFcq (canvassing, and refuting, various arguments against online pseudonymity and anonymity in light of Google+ decision).

[44] These are collectively known as "local shared objects." *See Local Shared Objects—"Flash Cookies,"* ELECTRONIC PRIVACY INFO. CENTER (July 21, 2005), https://epic.org/privacy/cookies/flash.html. For an extensive discussion of other forms of electronic identification see Tal Z. Zarsky & Norberto Nuno Gomes de Andrade, *Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum*, 74 OHIO ST. L.J. 1335 (2013).

[45] *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 361–63 (2009) (noting that because cloud services store content remotely, unless the content is encrypted the "cloud"-based location becomes another possible target for government surveillance without the user's knowledge).

chokepoints as a way to accomplish direct data acquisition about the activities of the intermediaries' customers.[46]

C. *Technological Counter-measures*

If neither behavioral nor contractual privacy-protective measures can in fact safeguard personal privacy, we would expect privacy-minded persons to turn to technology, especially when the technology offers privacy-enhancing tools that require neither changing one's daily habits nor attempting to negotiate contracts in the face of standard forms. These privacy enhancing tools range from simple things like drawing the curtains at home to much more exotic techniques designed to make it more difficult, even sometimes impossible, for others to capture data about personal actions and communications. For example, in order to foil CCTV, a person might dress in "stealth wear," clothing designed to protect against surveillance,[47] or might employ a laser designed to blind spy cameras.[48] Privacy-protective technical means employed online and on cell phones are often known as Privacy Enhancing Technologies (PETs). PETs have been defined as "a system of [Information Communication Technology] measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."[49] In 2007 the European Commission recommended that PETs "should be developed and more widely used, in particular where personal data are processed through information and communication technology (ICT) networks."[50] This Article concerns both PETs fitting the established definition, and also a related group of "privacy-protecting technologies." The super-set of

---

[46] *See* Barton Gellman & Todd Lindeman, *Inner Workings of a Top-Secret Spy Program*, WASH. POST, June 29, 2013, http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/; Jonathan Stray, *FAQ: What You Need To Know About the NSA's Surveillance Programs*, PROPUBLICA (June 27, 2013), https://www.propublica.org/article/nsa-data-collection-faq.

[47] *See* Jenna Wortham, *Stealth Wear Aims To Make a Tech Statement*, N.Y. TIMES, June 29, 2013, http://www.nytimes.com/2013/06/30/technology/stealth-wear-aims-to-make-a-tech-statement.html?smid=pl-share.

[48] *See* Loz Blain, *Anti-paparazzi Lasers Being Fitted to the World's Biggest Private Yacht*, GIZMAG (Sept. 22, 2009), http://www.gizmag.com/worlds-biggest-yacht-eclipse-roman-abramovich-anti-paparazzi-laser/12912/; *How To ZAP a Camera: Using Lasers To Temporarily Neutralize Camera Sensors*, MICHAEL NAIMARK (Oct. 2002), http://www.nai mark.net/projects/zap/howto.html. Note that under U.S. law deploying a laser in this fashion likely would be illegal, and certainly so if the laser were to cause any damage to equipment or persons.

[49] VAN BLARKOM, BORKING & OLK, *supra* note 4, at 33.

[50] *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy-Enhancing Technologies*, COM (2007) 228 final (May 2, 2007), *available at* http://europa.eu/legislation_summaries/information_society/data_protection/l14555_en.htm.

privacy-protecting technologies (PPT) includes PETs and also technologies that protect privacy but do not necessarily protect "the functionality of the information system"—rather, they intentionally impede systems designed to collect data in some manner. As discussed in the next section, however, many U.S. laws and industry rules make using many PPTs difficult or impossible.

III. ARE PETS ALLOWED?

U.S. law contains a number of provisions unfriendly to privacy, and the current administration seems to want more—not to mention the administration's role in the secret surveillance and data retention practices now coming to light. In addition, key communications intermediaries and key hardware manufacturers have chosen to make technological privacy self-help difficult or in some cases nearly impossible. Some of these private choices flow from legal rules or the fear of legal liability, but others appear to be primarily commercial decisions.

U.S. rules and big-firm practices limiting privacy technologies can be organized into four broad groups. The largest set of rules exist to ensure that users of private communications technologies are easily wiretapped or otherwise surveilled, in order to further the intelligence-gathering aims of the government, whether in service of national security agencies or of more ordinary law enforcement. These are discussed in Part III.A below.

A second, also substantial, set of rules consists of mandatory identification policies, some imposed by law, other by major communications intermediaries. These policies, surveyed in Part III.B, range widely across the law reflecting their divergent motivations; the detection of money laundering, terrorism financing, and other fraud is a notable sub-group.

A third group, discussed in Part III.C, places limits on hardware or software in order to serve some end such as reducing the likelihood of copyright infringement. As one common means of limiting both hardware and software involves embedding a unique identifier that the user cannot (or, if it is sufficiently obscure, is highly unlikely to) change, there is a degree of overlap between this category and mandatory ID policies.

The fourth, even more heterogeneous, group (Part III.D) encompasses rules that exist for reasons entirely independent of privacy or identity, but which suppress a particular privacy enhancing or privacy-protective technology more or less as an incident to the rule's primary purpose. For example, the tort rule that makes taking or harming another's property does not exist to limit privacy self-help, but it likely would make it a tort to use some anti-camera technologies.

A. *Mandating Surveillance-Friendly Technology and Data Retention*

U.S. law includes several provisions designed to provide access to private communications for intelligence agencies and law enforcement. Some of these

rules, such as the court-ordered warrant allowing the monitoring of a suspect's communications, have ancient roots and are largely uncontroversial. Similarly, the rule allowing the installation of a pen register[51] with a lesser court order[52] is also relatively uncontroversial—at least in its traditional application to telephony.

Examples of more controversial rules include the third-party doctrine mentioned above[53] and the requirement in the Communications Assistance for Law Enforcement Act (CALEA)[54] that telecommunications companies update their equipment to provide extensive built-in surveillance capabilities, allowing law enforcement agencies to monitor up to 20% of subscribers' transmissions in real time.[55]

Despite these and many other (overt) surveillance capabilities provided by law, the current administration appears unsatisfied. In 2011 the Obama Justice Department asked Congress to enact data retention legislation in the United States.[56] Later that year, the Judiciary Committee of the U.S. House of Representatives passed a wide-ranging data retention bill, labeling it the "Protecting Children from Internet Pornographers Act of 2011."[57] The proposal would require every "provider of an electronic communication service or a remote computing service" to retain the temporarily assigned network addresses the service assigns to each account for at least eighteen months, as well as account information about the customer.[58] As for the security aspects of this data, the proposed bill stated—non-bindingly—that "[i]t is the sense of Congress . . . that records retained pursuant to section 2703(h) of title 18, United States Code, should be stored securely to protect customer privacy and prevent against breaches of the records."[59] That said, the text then goes on to state that the covered providers shall have no liability for any disclosure of the

---

[51] A pen register is a means of recording the phone numbers called by a phone line being monitored and the length of the conversation, but does not give access to the content of the communication. *See* Smith v. Maryland, 442 U.S. 735, 741–42 (1979) (comparing pen register to full wiretap).

[52] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1851 (codified at 18 U.S.C. §§ 2510–2522).

[53] *See supra* text accompanying notes 37–39.

[54] 47 U.S.C. §§ 1001–1010 (2012).

[55] *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 421–24 (2012), *available at* http://www.stlr.org/cite.cgi?volume=13&article=9.

[56] *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 6–7 (2011) (statement of Jason Weinstein, Deputy Assistant Attorney General), *available at* http://judiciary.house.gov/hearings/pdf/Weinstein01252011.pdf.

[57] *See* H.R. REP. NO. 112-281, pt. 1, at 2 (2011).

[58] *See id.* (amending 18 U.S.C. § 2703); *see also* Declan McCullagh, *House Panel Approves Broadened ISP Snooping Bill*, CNET NEWS (July 28, 2011, 1:41 PM), http://news.cnet.com/8301-31921_3-20084939-281/house-panel-approves-broadened-isp-snooping-bill/.

[59] H.R. REP. NO. 112-281, at 2.

information.[60] Alarmingly, the statute also permits non-judicial "administrative subpoenas" by the U.S. Marshals service, albeit limiting that new power to investigations of "an unregistered sex offender."[61]

More recently, the Obama Administration floated "CALEA II," a proposal that some or all cell phone application providers should be subject to CALEA rules requiring them to be "wiretap friendly."[62] Ironically—in light of subsequent revelations of NSA data collection—the FBI argued that it was "going dark," that is, losing the ability to wiretap every conversation.[63] Presumably the FBI's concern was with applications such as RedPhone, which allows Android phone users to have an encrypted phone conversation[64] (in my experience, at the cost of some call quality) via a so-called "endpoint to endpoint" encryption. According to an eminent group of cryptographers who critiqued the FBI proposal, its effects not only would be largely ineffective, but would create serious security risks for users of endpoint-to-endpoint encryption tools.[65]

The United States' publicly acknowledged privacy-unfriendly rules may, alas, be no more than the tip of the iceberg. In addition to the public face of drift-net surveillance, U.S. (not to mention non-U.S.) persons face the specter of secret surveillance. If recent revelations about the NSA are accurate,[66] at the same time as the Obama Administration was asking for additional data retention authority, it was secretly asserting that it already had all the legal authority needed to demand that ISPs and cell phone companies turn over a substantial amount of data about their customers' communications—the "metadata" recording who phoned, messaged, or emailed whom, where, and for how long.[67] Whether, and to what extent, phone and message traffic content is or was warehoused or analyzed remains unclear, although it appears to include e-mails, Internet telephony, and Internet video.[68] There is also a report that the NSA stores the full content of telephone calls.[69] In any case, we do know that in at

---

[60] *Id.* at 3.

[61] *Id.* at 4.

[62] *See* BEN ADIDA ET AL., CTR. FOR DEMOCRACY & TECH., CALEA II: RISKS OF WIRETAP MODIFICATIONS TO ENDPOINTS 2 (May 17, 2013), *available at* https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

[63] *Id.*

[64] *See RedPhone*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone&hl=en (last visited Aug. 10, 2013).

[65] *See* ADIDA ET AL., *supra* note 62, § 3, at 4–7.

[66] *See* Greenwald, *supra* note 46; *see also supra* note 39.

[67] For a summary of what was known at the time this was written see Gellman & Lindeman, *supra* note 46; Stray, *supra* note 46.

[68] Gellman & Lindeman, *supra* note 46.

[69] *See* Siobhan Gorman & Jennifer Valentino-Devries, *New Details Show Broader NSA Surveillance Reach: Programs Cover 75% of Nation's Traffic, Can Snare Emails*, WALL ST. J., Aug. 20, 2013, http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html (attributing information to interviews with "current and former officials"); Kevin Gosztola, *Glenn Greenwald's Speech to the Socialism Conference [with Transcript]*,

least some cases the NSA shared data with domestic law enforcement agencies when it collected evidence of a crime.[70]

Persons seeking to protect their privacy in this environment can either stop using the technologies being surveilled—hardly a practical option for many—or can try to protect their communications by technical means such as encryption.[71] U.S. export control policy, however, has the not-unintended effect of discouraging equipment and software manufacturers from building meaningful encryption into their products.[72] At present, the major email programs, the major video conference programs, and all mass-market cellphone handsets, default to sending messages without encryption. While it is possible for a determined user to add in encryption,[73] at least in my experience it is not easy to configure encryption software well, and in any case it only works if the person you are communicating with uses a compatible product.

B. *Mandatory Identification*

One particularly effective way for a person to safeguard his or her privacy is to remain anonymous. By remaining anonymous a person ensures that his or her communications, transactions, and movements cannot be linked to their author—and perhaps not even to each other. Unfortunately for anyone hoping to stay anonymous, many U.S. legal rules, and also many corporate policies in the ICT sector, make it difficult to be anonymous.

Financial intermediaries must, as noted above, verify their customers' identities,[74] which has the effect of tying online transactions to an identity (as distinguished from an in-person cash transaction or, perhaps, a Bitcoin transaction).[75] Anti-anonymity rules extend far beyond transactions. In order to

---

DISSENTER (June 29, 2013, 9:47 AM), http://dissenter.firedoglake.com/2013/06/29/glenn-greenwalds-speech-to-the-socialism-conference-with-transcript (quoting Glenn Greenwald referring to unpublished NSA document).

[70] Kim Zetter, *5 Fun Facts from the Latest NSA Leak*, WIRED (June 20, 2013, 6:04 PM), http://www.wired.com/threatlevel/2013/06/five-fun-facts-on-the-nsa-leak/.

[71] *Cf.* Pete Ashdown, *The NSA and XMission*, TRANSMISSION (June 10, 2013), https://transmission.xmission.com/2013/06/10/the-nsa-and-xmission (ISP operator's statement that "[t]he Internet was built on trust, and nobody anticipated interception of data would be a problem. The only way to fix this is through encryption." (emphasis omitted)).

[72] *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 748–51 (1995) [hereinafter Froomkin, *Metaphor*]; A. Michael Froomkin, *It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL. F. 15, 43–50 [hereinafter Froomkin, *Planet Clipper*].

[73] *E.g.*, *OpenPGP Encryption for Webmail*, MAILVELOPE, http://www.mailvelope.com/ (last visited Nov. 9, 2013) (for Gmail users).

[74] *See supra* text accompanying notes 35–36.

[75] Bitcoin is an anonymous online e-payment mechanism. Bitcoins are on the borderline of U.S. anti-money-laundering law. The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) classifies users of virtual currencies such as Bitcoin as outside the definition of a "money services business" (MSB) and thus not subject to know-

provide more precise location information to 911 dispatchers, cell phone companies are required to fix the location of cell phone users at all times to within 150 meters.[76] The location of cell phone users becomes a private record held by the cell phone service provider, discoverable and perhaps even routinely obtained by the government,[77] and cell phone companies are forbidden from competing to provide a more private, if perhaps less ambulance-ready, service.[78]

As the need for privacy-enhanced communications increases, and as email and computer-mediated phone and video become increasingly significant means of communication, the computer hardware on which those communications take place is less and less hospitable to strong privacy. Delineating the role of U.S. law in this evolution requires a short detour into intellectual property law because copyright protection has been a significant motivation for this shift. General-purpose computers, and increasingly other media-players, make digital copying easy. In an attempt to protect copyright holders, Congress enacted the Digital Millennium Copyright Act (DMCA). Among its provisions, the DMCA criminalizes making available technologies whose primary purpose and function are to circumvent content protection technologies.[79] As a result, copy-protection measures, notably "digital rights management" (DRM) technologies,

---

your-customer regulations. On the other hand, FinCEN treats Bitcoin brokers who exchange Bitcoins for cash as subject to know-your-customer and other rules. *See* DEP'T OF THE TREASURY FIN. CRIMES ENFORCEMENT NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1–2 (2013), *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf. The extent to which Bitcoin protects identity against a government is debatable. Apparently, "an agency with subpoena power would be well placed to identify who is paying money to whom" in the Bitcoin network. Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 2 (unpublished manuscript), *available at* http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

[76] 911 Service, 47 C.F.R. §§ 20.18(b), (h)(2)(i) (2012). *See generally* Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308 (2004).

[77] The U.S. government denied that the United States requires cell phone providers to turn over all the location information providers have on their customers. *See* Matt Pearce, *NSA Does Not Collect Cellphone Location Data, Officials Say*, L.A. TIMES, June 24, 2013, http://www.latimes.com/news/nation/nationnow/la-na-nn-nsa-phone-location-data-20130624,0,6266092.story. The denial came hedged with enough evasions and caveats to make surveillance experts suspicious. *See id.*; *cf.* Jameel Jaffer & Brett Max Kaufman, *How To Decode the True Meaning of What NSA Officials Say*, SLATE (July 31, 2013, 5:29 PM), http://www.slate.com/articles/news_and_politics/politics/2013/07/nsa_lexicon_how_james_clapper_and_other_u_s_officials_mislead_the_american.html ("When it comes to discussing government surveillance, U.S. intelligence officials have been using a vocabulary of misdirection—a language that allows them to say one thing while meaning quite another.").

[78] *Cf.* 47 C.F.R. § 20.18 (requiring that providers report location of cell phone users making 911 calls at a required degree of accuracy).

[79] Digital Millennium Copyright Act § 103(a), 17 U.S.C. §§ 1201–1202, 1204 (2012).

acquired legal protection from circumvention.[80] The legal protection of DRM is significant to privacy protection because DRM exists to distinguish between authorized users of content (who have presumably purchased or otherwise acquired a license) and other, unlicensed, users. Thus, in order to access a work, the user must present a digital license—one that is usually unique, and frequently traceable to the user.[81] From the copyright-holder's perspective, DRM provides a short-term advantage but carries the risk of long-term vulnerabilities, notably that if the DRM scheme is ever broken—e.g. reverse engineered so that users can trick it into believing they are authorized—there is little if anything that can be done to again secure copies now vulnerable to copying and unlicensed use. Furthermore, there was and is every reason to believe that real-life DRM will be broken.[82] The DMCA sought to fill this gap by making it illegal to share the tools which could be used to unlock DRM-protected content.[83] In so doing, however, it also made it illegal to share tools that might allow users of DRM-protected content to use their licensed content without having to identify themselves.

A similar progression is under way in hardware. Under the so-called "Trusted Computing" initiative, chip-makers are placing unique identifiers on computer chips that can be invoked by software to identify the machine, without the knowledge or consent of the user.[84] Intel's latest generation of chips, Sandy Bridge, includes a unique identifier (they call it the "Intel Insider") just waiting for software—not necessarily under the control of the user—to identify it.[85] The hope, not yet realized, is that having this capability will give more content providers the courage to stream top-quality movies online because they can encrypt it in a way that only a chip equipped with a unique identifier will be able to decrypt.[86] Of course, every Internet-connected device already has a

---

[80] *See* Bill D. Herman, *A Political History of DRM and Related Copyright Debates, 1987–2012*, 14 YALE J.L. & TECH. 162, 180–81 (2012).

[81] *See, e.g.*, *DRM Individualization*, MICROSOFT (June 12, 2013), http://msdn.microsoft.com/en-us/library/windows/desktop/dd757083%28v=vs.85%29.aspx.

[82] *See* Bruce Schneier, *The Futility of Digital Copy Prevention*, CRYPTO-GRAM NEWSL. (May 15, 2001), http://www.schneier.com/crypto-gram-0105.html#3.

[83] *See* 17 U.S.C. § 1201(a)(2).

[84] By 2006 most major computer manufacturers were shipping systems that included Trusted Platform Modules support although in many cases the user could turn them on or off in the BIOS. *Trusted Platform Module*, NOVARA (Mar. 26, 2006), http://www.novara-software.com/windows-vista/lista-da-evitare.php. These modules are in most computers sold today. *See* Cory Doctorow, *The Coming Civil War over General Purpose Computing*, BOINGBOING (July 2012), http://boingboing.net/2012/08/23/civilwar.html.

[85] *See* Richard Adhikari, *Intel Builds Sandy Bridge with a DRM Tollbooth*, TECHNEWSWORLD (Jan. 4, 2011, 5:00 AM), http://www.technewsworld.com/story/71568.html?wlc=1315966732; Nick Knupffer, *Intel Insider—What Is It? (Is It DRM? And Yes It Delivers Top Quality Movies to Your PC)*, TECHNOLOGY@INTEL BLOG (Jan. 4, 2011), http://blogs.intel.com/technology/2011/01/intel_insider_-_what_is_it_no.php.

[86] Brooks Barnes, *In This War, Movie Studios Are Siding with Your Couch*, N.Y. TIMES, Sept. 25, 2010, http://www.nytimes.com/2010/09/26/business/26steal.html. This technology was designed to "control users and limit the abilities of computers." Chad

unique MAC number, which also can be used to uniquely identify devices, but these are usually part of a peripheral device. It is easier to replace or mask a peripheral than it is to change or mask something hardwired on the CPU.[87]

There is no hardware equivalent to the DMCA; chip makers are deploying the "Trusted Computing" project without the spur of a direct legal mandate. Part of the motivation may be the belief that consumers will prefer devices that may be able to access a wider variety of content.[88] Another motivation, however, appears to have been the manufacturers' fear that unless they deployed something designed to prevent unlicensed copying, Congress would impose on them something akin to the DMCA.[89] Law can thus cast a shadow on privacy-enhancing technology even when it is only hypothetical. As a consequence of the technological choices of hardware and software manufacturers, the DMCA's protection of DRM against circumvention results in disempowering the user. One consequence of those technologies is that if users want to do certain things with their machines—play popular movies for example—they are not able to install tools that protect their privacy against metering and monitoring by the firms using DRM.

As Jonathan Zittrain has noted, primarily commercial concerns can suffice to motivate architectural choices that centralize control over user behavior.[90] Take, for example, Apple's decision to allow the iPhone to run only Apple-approved software. On the one hand, this strong "curation" will tend to protect users from malicious applications such as Trojan horses and viruses. On the

---

Woodford, Comment, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, 75 U. COLO. L. REV. 253, 280 (2004) (citation omitted); *see also* Ryan Roemer, *Locking Down Loose Bits: Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, 2003 UCLA J.L. & TECH. 1, 4–6.

[87] *See, e.g.*, *How To Change a MAC Address*, TECH-FAQ, http://www.tech-faq.com/how-to-change-a-mac-address.html (last updated Dec. 11, 2012). Interestingly, the default behavior in Windows 7 is to use a randomized substitute for the MAC address. *See* Scott Hogg, *Windows 7 IPv6 Support*, NETWORK WORLD (Jan. 29, 2009, 11:15 AM), http://www.networkworld.com/community/node/37947. This option is permitted by T. NARTEN ET AL., RFC 4941, PRIVACY EXTENSIONS FOR STATELESS ADDRESS AUTOCONFIGURATION IN IPV6 (Sept. 2007), *available at* http://www.ietf.org/rfc/rfc4941.txt, but has not been widely adopted elsewhere. In contrast, the current versions of Apple iOS and Android are shipping with privacy extensions turned off. *See IPv6: Smartphones Compromise Users' Privacy*, H SECURITY (Jan. 14, 2011, 2:41 PM), http://www.h-online.com/security/news/item/IPv6-Smartphones-compromise-users-privacy-1169708.html. I am indebted to CDT Chief Computer Scientist Alissa Cooper for this information.

[88] *See, e.g.*, Jonathan Weinberg, *Hardware-Based ID, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251, 1257–58 (2000) (discussing but rejecting claim that consumers will benefit from technological copyright controls); Fred Koenigsberg, *The Fifth Annual Christopher A. Meyer Memorial Lecture: Humpty-Dumpty in Copyrightland*, 51 J. COPYRIGHT SOC'Y U.S.A. 677, 687–88 (2004) (endorsing view that "in the long run the general public will be the heaviest loser if copyright is weakened" (citation omitted)).

[89] *See* Roemer, *supra* note 86, at 57.

[90] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 101–26 (2008).

other hand, it also prevents the iPhone's user from installing any privacy enhancing software not approved by Apple.

In the United States, the government has not sought to make anonymity illegal or to require online identification directly. Indeed, a legal requirement that persons identify themselves online would not only be controversial but would likely be unconstitutional.[91] Most Internet and also cell phone communications originate from devices that are linked to a user by the service provider; access control and identification are required for billing purposes and out of fear that unidentified persons might hack or otherwise harm the system. Identification is thus something of a default for commercial reasons, and for security reasons, even in non-profit settings.[92] As the United States has no European-style Data Protection Directive to act as a counterweight to the private retention of data, the users' needs for a technological defense against being identified and profiled is even more acute and the issue is to what extent users will remain able to use privacy-protecting technologies to change the default and mask their identity. On this question, the U.S. government appears to be pursuing contradictory policies, some of which might enhance anonymous communication while others seem calculated to make it difficult or impossible.

The Commerce Department's *National Strategy for Trusted Identities in Cyberspace*[93] epitomizes one side of the division. The *Strategy* envisions an "Identity Ecosystem" described as a system that will enhance privacy and civil liberties:

> The Identity Ecosystem will use privacy-enhancing technology and policies to inhibit the ability of service providers to link an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace. By default, only the minimum necessary information will be shared in a transaction. For example, the Identity Ecosystem will allow a consumer to provide her age during a transaction without also providing her birth date, name, address, or other identifying data.
>
> In addition to privacy protections, the Identity Ecosystem will preserve online anonymity and pseudonymity, including anonymous browsing.[94]

While setting out the outlines of how such a system might work in theory, the *Strategy* does not attempt to explain key aspects of how its ambitious goals might be attained in practice. Instead it sets out a ten-year roadmap, in which

---

[91] *See* A. Michael Froomkin, *Anonymity and the Law in the United States*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 441, 442–47 (Ian Kerr ed., 2009).

[92] Fear of spammers using resources to send large numbers of messages is one such fear. The spam not only can strain the network, but can cause recipient networks to blacklist the sending organization, thus further interfering with legitimate traffic.

[93] THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[94] *Id.* at 2.

the first three to five years require "standardization of policy and technology."[95] The key to implementations, we are told, rests on the twin pillars of underlying reliable offline credentials[96] and private-sector leadership:

> Ultimately, the Identity Ecosystem can only be designed and built by the private sector. The Federal Government will support the private sector, ensure that the Identity Ecosystem respects the privacy and otherwise supports the civil liberties of individuals, and be a leader in implementing the Identity Ecosystem in its own services. Existing efforts by the public and private sectors have already established services that are significant components of the Identity Ecosystem, but much remains to be done. Individuals, businesses, non-profits, advocacy groups, associations, and all levels of government must work in partnership to improve how identities are trusted and used in cyberspace.[97]

Only one month later, however, the White House released its *International Strategy for Cyberspace*, a document that while it also extolled the Internet's benefits and opportunities, warned darkly of its dangers:

> Extortion, fraud, identity theft, and child exploitation can threaten users' confidence in online commerce, social networks and even their personal safety. The theft of intellectual property threatens national competitiveness and the innovation that drives it. These challenges transcend national borders; low costs of entry to cyberspace and the ability to establish an anonymous virtual presence can also lead to "safe havens" for criminals, with or without a state's knowledge. Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace.[98]

Rather than commit to protecting anonymity, this policy document suggested that while privacy was important, the main goals were notice and the active role of government to protect users from evils while subject to "judicial review and oversight."[99] Thus, the Internet of the future should be "secure"—in the sense of not allowing bad actors free rein, rather than in the sense of

---

[95] *Id.* at 40.

[96] *Id.* at 8 ("The Strategy does not explicitly address identity and trust issues in the offline world; however, offline and online identity solutions can and should complement each other. Identity proofing (verifying the identity of an individual) and the quality of identity source documents have a profound impact on establishing trusted digital identities, but the Strategy does not prescribe how these processes and documents need to evolve." (emphasis omitted)).

[97] *Id.* at 43.

[98] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 4 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[99] *Id.* at 5.

fostering communications free from third-party monitoring or accountability.[100] Fundamental values of freedom of expression and privacy (defined as freedom from "arbitrary or unlawful" state action) would be balanced against "respect [for] intellectual property rights" and "protection from crime."[101]

C. *Technology-Limiting Rules*

As the *International Strategy for Cyberspace* demonstrates, U.S. policy typically treats privacy as a value to be traded off against other benefits, notably safety and security. This is particularly evident in regards to ICT privacy, but also applies more generally. A concern with safety, perhaps leavened with some solicitude for liability in accident cases, led the National Highway Safety Administration to propose a rule requiring event vehicle recorders (also known as "black boxes") in all cars; if the rule becomes final, car makers will not be able to compete on driver privacy.[102]

As noted above, cell phones report fine-grained user location;[103] firms want access to this information in order to know exactly where their potential customers are and what they are looking at, a desire being filled by systems such as the Euclid Analytics monitoring system.[104] At present, the only way consumers who own cell phones can defend themselves against being tracked as they shop is to turn off their cell phones,[105] or to create bad publicity for retailers who use tracking technology. Nordstrom recently abandoned its customer tracking days after it became public, demonstrating that public

---

[100] *See id.* at 8 ("Our Goal" is "an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace." (emphasis omitted)).

[101] *Id.* at 10.

[102] The Notice of Proposed Rulemaking speaks only of safety and research. *See* Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74144, 74145 (proposed Dec. 13, 2012) (to be codified at 49 C.F.R. pt. 571) ("to improve crash and defect investigation and crash data collection quality to assist safety researchers, vehicle manufacturers, and the agency to understand vehicle crashes better and more precisely").

[103] *See supra* text accompanying note 76.

[104] *See* Angela Martin, *Nordstrom Using Smart Phones To Track Customers Movements*, CBS DFW (May 7, 2013, 10:05 PM), http://dfw.cbslocal.com/2013/05/07/nordstrom-using-smart-phones-to-track-customers-movements/; *see also* Quentin Hardy, *Technology Turns to Tracking People Offline*, N.Y. TIMES BITS BLOG (Mar. 7, 2013, 2:52 PM), http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline/ (reporting that Euclid has used fifty million customers' smart phones in 4,000 locations to monitor "how many people are coming into a store, how long they stay and even which aisles they walk").

[105] *See* Martin, *supra* note 104.

information about the use of monitoring technology will deter its use in at least some cases.[106]

Online, the choices are especially stark. Even if it is the case that the NSA is collecting all user meta-data for Internet and telephone calls, and also retaining copies of many or all communications,[107] users of telephones and computers still have an interest in protecting themselves from non-governmental parties who would like to know things about them. This is increasingly difficult, and in some environments pretty near impossible. To begin with, the architecture of the Internet makes certain types of identification routine. Every Internet communication requires an Internet Protocol (IP) number.[108] While in some cases it is possible to mask this number when sending data, anyone hoping to receive information must provide an accurate and unique IP address or that information will not be received.[109] If, as is pretty much always the case, IP numbers are permanent or, when shared, ISPs and other intermediaries keep records of who has which IP number at what time, the IP number becomes a way of identifying most speakers and almost all listeners.[110] "Almost all" because it is possible, with some effort, to mask one's identity with the help of an intermediary. Even without the cooperation of the sender's ISP, the very IP number itself usually discloses important geo-location information about the sender.[111]

We have seen how Ixquick offers this masking service in the search engine market; cognate proxy services exist for the web and for email, but they add complexity and usually noticeable delay to any Internet usage.[112] While Tor and other proxy services do not protect against wiretaps and other forms of observation at the customer's ISP, they do anonymize the user as regards the party on the other end of the communication.[113] At present there are no U.S. legal restrictions on the use of these proxies, just practical ones.

---

[106] *See* Angela Martin, *Nordstrom No Longer Tracking Customer Phones*, CBS DFW (May 9, 2013, 10:43 PM), http://dfw.cbslocal.com/2013/05/09/nordstrom-no-longer-tracking-customer-smart-phones/.

[107] *See supra* note 46.

[108] *See* Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J 567, 594 (2012).

[109] *See id.*

[110] *See id.* at 595.

[111] *See id.* at 596–99.

[112] *See, e.g.*, Prithula Dhungel et al., Waiting for Anonymity: Understanding Delays in Tor, at pt. 1 (unpublished manuscript), *available at* http://cis.poly.edu/~ross/papers/Tor.pdf. *But see* Roger Dingledine & Steven J. Murdoch, *Performance Improvements on Tor or, Why Tor Is Slow and What We're Going To Do About It*, TOR BLOG (Mar. 11, 2009), https://svn.torproject.org/svn/projects/roadmaps/2009-03-11-performance.pdf.

[113] Dingledine & Murdoch, *supra* note 112, at 1.

D. *Other Side Effects*

Many laws which exist, and often long have existed, for legitimate social purposes have the unintentional effect of making the deployments of modern PETs difficult or impossible. This section provides a small number of representative examples.

On August 6, 2013, the Board of Deer Trail Colorado considered a symbolic ordinance that would have created "drone hunting licenses" and bounties for shooting unmanned drones.[114] The Board split 3-3, meaning that the issue will be put to a referendum this November.[115] Leaving aside Supremacy Clause issues (the ordinance was aimed at federally owned and operated unmanned air vehicles), the inspiration for the proposed ordinance illustrates a key difficulty facing most self-help measures against surveillance: any defensive action that damages a legally emplaced surveillance device,[116] whether public or private, is likely both illegal and tortious primarily due to criminal and property rules that exist to regulate conduct which has nothing to do with privacy. As the law now stands—that is, in the absence of unlikely new enabling legislation—only purely passive defenses against surveillance, and not even all of these, are likely to be legal.[117]

---

[114] The ordinance states, in part,

> The Town of Deer Trail shall issue a reward of $100 to any shooter who presents a valid hunting license and . . . identifiable parts of an unmanned aerial vehicle whose markings and configuration are consistent with those used on any similar craft known to be owned or operated by the United States federal government.

Amanda Kost, *Deer Trail Town Board Has Tie Vote on Drone-Hunting Proposal, Sending Issue to Town To Vote in Nov.*, ABC 7 NEWS (Aug. 6, 2013), http://www.thedenverchannel.com/news/local-news/town-board-in-tiny-deer-trail-colo-votes-tonight-on-proposed-drone-hunting-licences-bounties.

[115] *Id.*

[116] The legality of low-altitude drone flights over private property likely turns in the first instance on the applicability and reach of FAA regulations. *See generally* Timothy M. Ravich, *The Integration of Unmanned Aerial Vehicles into the National Airspace*, 85 N.D. L. REV. 597 (2009) (surveying issues about application and validity of current FAA rules as applied to drones). Absent a regulatory permission, a drone flying low over private property would constitute a trespass. *See* Alexis C. Madrigal, *If I Fly a UAV over My Neighbor's House, Is It Trespassing?*, ATLANTIC (Oct. 10, 2012, 2:00 PM), http://www.theatlantic.com/technology/archive/2012/10/if-i-fly-a-uav-over-my-neighbors-house-is-it-trespassing/263431/.

[117] Fear of drone overflights has spurred legislation in at least seven states: Florida, *see* Freedom from Unwarranted Surveillance Act, ch. 2013-33, 2013 Fla. Laws 33 (no right to self-help; an aggrieved party may seek injunctive or pecuniary relief); Idaho, *see* Act of Apr. 11, 2013, ch. 328, 2013 Idaho Sess. Laws 328 (no right to self-help; an aggrieved party may seek injunctive or pecuniary relief); Illinois, *see* Freedom from Drone Surveillance Act, 2013 Ill. Pub. Act 98-0569 (no right to self-help), Act of Aug. 16, 2013, 2013 Ill. Pub. Act 98-0402 (criminalizing use of drones to interfere with another's lawful taking of wildlife or aquatic life); Montana, *see* Act of May 1, 2013, ch. 377, 2013 Mont. Laws 377 (no right to

Consider, for example, the "Camera Zapper," a laser-based system designed to blind surveillance cameras.[118] Even assuming that the zapper's laser did not itself violate any local ordinances, it surely would be a tort to damage the camera in any way. Permanent damage would be conversion; temporary harm would be trespass to chattel. Depending on the jurisdiction, the same acts might be considered vandalism, criminal mischief, criminal trespass or various other crimes or violations. These tort and criminal rules exist for valid reasons having nothing to do with PETs, but their existence means that a variety of (perhaps slightly exotic) privacy self-help techniques are unavailable to the law-abiding citizen.

In some cases, it may be illegal to attempt to foil the cameras even passively. It is usually illegal to obscure one's license plate, leaving cars vulnerable to an extensive network of automated license-plate monitors.[119] Several states have statutes prohibiting the wearing of masks in public areas,[120] and federal law prohibits wearing masks for certain purposes.[121] State anti-mask laws arose primarily in response to the actions of the Ku Klux Klan.[122] These laws have survived many challenges.[123] Employees who seek to block

---

self-help); Tennessee, *see* Freedom from Unwarranted Surveillance Act, ch. 470, 2013 Tenn. Pub. Acts 470 (no right to self-help; an aggrieved party may seek injunctive or pecuniary relief); Texas, *see* Texas Privacy Act, ch. 1390, 2013 Tex. Gen. Laws 1390 (no right to self-help; an aggrieved party may seek injunctive or pecuniary relief; various privacy invasions are criminalized); Virginia, *see* Act of Apr. 3, 2013, ch. 755, 2013 Va. Acts 755 (no right to self-help).

[118] For details see NAIMARK, *supra* note 48.

[119] For example, Virginia forbids mounting anything around a license plate that alters or obscures it. VA. CODE ANN. § 46.2-716 (2013). Similarly, Pennsylvania law states that "[i]t is unlawful to display on any vehicle a registration plate which: . . . (2) is obscured in any manner which inhibits the proper operation of an automated red light enforcement system . . . ; (3) is otherwise illegible at a reasonable distance or is obscured in any manner." 75 PA. CONS. STAT. ANN. § 1332 (2012). On license plate monitors, see generally CATHERINE CRUMP ET AL., ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 13–16 (July 17, 2013), *available at* http://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record (noting millions of records being retained indefinitely).

[120] For a full survey see Margot Kaminski, *Real Masks and Real Name Policies: Applying Anti-mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815, 848–49 (2013). These statutes generally bar the donning of any facial covering that alters the appearance of the wearer, making him unidentifiable or causing fear or intimidation in other persons. *See, e.g.*, DEL. CODE ANN. tit. 11, § 1301 (2012); LA. REV. STAT. ANN. § 14:313 (2013); N.Y. PENAL LAW § 240.35 (McKinney 2013).

[121] 42 U.S.C. § 1985(3) (2012) (creating cause of action "[i]f two or more persons in any State or Territory conspire or go in disguise on the highway or on the premises of another, for the purpose of depriving, either directly or indirectly, any person or class of persons of the equal protection of the laws, or of equal privileges and immunities under the laws").

[122] *See* Kaminski, *supra* note 120, at 848.

[123] *See* Church of the Am. Knights of the Ku Klux Klan v. Kerik, 356 F.3d 197, 208 (2d Cir. 2004) (upholding New York anti-mask law against First Amendment challenge); West Virginia v. Berrill, 474 S.E.2d 508, 514 (W. Va. 1996) (finding a legitimate government

employer-installed GPS trackers may face tens of thousands of dollars in fines for interfering with other legitimate GPS-based systems.[124]

Perhaps the most notorious set of legal rules that served to block PETs were the United States' longstanding restrictions on the exportation of cryptographic software and hardware. Although it was legal to use strong cryptography in the United States, export of strong encryption was for many years a serious offense.[125] As a result, major firms such as Microsoft chose not to build strong cryptography into email and word processing programs because that would have required them to produce different versions for the U.S. and non-U.S. markets.[126] Not only would this have required maintaining a more complex codebase, but the firms feared that non-U.S. customers would, with some reason, feel like they were being sold a second-class product. The U.S. government eventually relaxed its cryptography regulations somewhat, but only after a long rearguard action designed to prevent the spread of strong(ish) cryptography as long as possible.[127] That side effect may have originally been unintentional, but the U.S. government certainly took full advantage of it for many years.

Furthermore, the side-effect problem is not limited to existing rules. Proposed solutions to technology-based social problems can create new anti-PET side effects. For example, some public officials have called on cell phone manufacturers to make cell phone theft more difficult by making it impossible to change the cell phone's unique identifier, the International Mobile Station Equipment Identity (IMEI).[128] Blocking IMEI masking would make it harder to hide cell phone theft, but do so at the cost of preventing users from changing the IMEI to baffle any tracking operation relying on it.[129] (Users also may want to change an IMEI in order to sell a cell phone as some carriers would otherwise attempt to block the sale or refuse to route calls to the phone after it changed hands.)

---

interest in the protection of citizens from the violence, fear, and intimidation of being confronted by someone whom they cannot identify).

[124] *See N.J. Man in a Jam, After Illegal GPS Device Interferes with Newark Liberty Operations*, CBS2 NEW YORK (Aug. 9, 2013, 5:43 PM), http://newyork.cbslocal.com/2013/08/09/n-j-man-in-a-jam-after-illegal-gps-device-interferes-with-newark-liberty-operations/ (reporting FAA fined employee of construction company $32,000 for his use of $100 GPS-blocker he intended "to hide his movements from his boss" but which interfered with test of new airport GPS system).

[125] *See* Froomkin, *Planet Clipper*, *supra* note 72, at 18–20.

[126] *See id.*

[127] *See id.* at 748–51; Froomkin, *Metaphor*, *supra* note 72, at 21–23.

[128] *See* Brian X. Chen & Malia Wollan, *Cellphone Thefts Grow, but the Industry Looks the Other Way*, N.Y. TIMES, May 1, 2013, http://www.nytimes.com/2013/05/02/technology/cellphone-thefts-grow-but-the-industry-looks-the-other-way.html (quoting George Gascón, San Francisco's district attorney, as saying, "Unlike other types of crimes, this is a crime that could be easily fixed with a technological solution").

[129] *See id.* (quoting Electronic Frontier Foundation Senior Staff Technologist Seth Schoen who described the right to change the identification as a "pro-privacy measure").

IV. CONCLUSION: BE NICE TO PETS

Given the increasing number of ways in which privacy is under assault, given the increase of ID theft, and given the conventional wisdom that consumers are responsible for securing their privacy themselves, one might reasonably expect that U.S. industry and the U.S. government would encourage the development and deployment of both PETs and PPTs—particularly as other forms of self-help privacy protection, notably changes in habits or attempts to secure contractual privacy protections, seem so unlikely to be effective.[130] Unfortunately, the truth is much closer to the reverse: a plethora of commercial practices and legal rules discourage privacy-protective technologies, or even make them illegal. Many, perhaps most, of these rules were not designed with PETs in mind; rather, they serve some other goal, and the obstacle to PPT deployment and use is a side-effect, incidental damage. The cumulative effect of these disparate policies, however, is to create a climate in which PET use remains difficult—and thus stunted. In the United States, a combination of public and private efforts have made it unnecessarily difficult, and in some cases risky, illegal, or even impossible, for consumers to install and use a wide variety of defenses to both online and offline surveillance.

As visible surveillance grows, and especially as we learn more and more about the invisible surveillance to which we daily are subjected—with or without the approval of a secret court—we more urgently need laws that default to privacy, or at least make it practicable for people to choose a privacy option. Instead of being nurtured and encouraged, too often privacy-enhancing technology is discouraged, or PETs are not allowed, or worse their use is criminalized. Instead of putting PETs on a leash, we should say, "PETs Welcome!"

V. UPDATE: RETHINKING PETS AFTER SNOWDEN

As this Article went to press, reporters working with former NSA contractor Edward Snowden continued to release new information describing the NSA's systematic subversion of encryption and other privacy enhancing technologies.

One might therefore ask how many of the various obstacles to the deployment of PETs and other privacy protective technologies described in this Article are not, as is sometimes suggested above, the result of malign coincidence or collateral damage from an over-aggressive focus on some other objective, but rather part of a plan to systematically neuter PETs and make computer (and cellphone) aided communication and storage a privacy-free zone, at least as regards U.S. government monitoring.

---

[130] A fourth option would be national privacy legislation; however, even in a more privacy-friendly regulatory climate, there likely would remain people who would choose to employ PETs for additional privacy and security—if the PETs were available and legal.

We now have evidence that a covert element of the U.S. government, the NSA, ran a program approved at high levels that consciously subverted key encryption technologies and bypassed others in order to make it as difficult as possible for U.S. residents to protect their informational privacy. Evidence has now emerged that the NSA quietly introduced vulnerabilities known only to it in international cryptography standards intended for the Internet and for smartphones.

> Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own 'back door' in all encryption, it set out to accomplish the same goal by stealth.[131]

Meanwhile, acting both with and without the consent of major software manufacturers, the NSA introduced secret back doors into widely-used commercial software. Specifically,

> companies say they were coerced by the government into handing over their master encryption keys or building in a back door. And the agency used its influence as the world's most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world.[132]

The result is to substantially undermine PETs on which millions of U.S. residents rely daily including Secure Sockets Layer (SSL) used for an increasing fraction of World Wide Web access, virtual private networks (VPNs), and the encryption standard used on fourth-generation, or 4G, smartphones.[133]

Similarly, the NSA induced key Internet communications intermediaries to give the NSA back door access to users' communications, most commonly meaning that the NSA could copy pre-encrypted text. Among the companies reported to have cooperated was Microsoft, for email systems Outlook and Hotmail, video conference system Skype, and cloud storage system SkyDrive.[134] Apple,[135] Google, Yahoo, and Facebook were also targeted.[136] As

---

[131] Nicole Perlroth, Jeff Larson & Scott Shan, *N.S.A. Able To Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all.

[132] *Id.*

[133] *Id.*

[134] *See* Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages*, GUARDIAN, July 11, 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

[135] Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

a result, the NSA (and the UK's GCHQ) could in effect circumvent even the strong encryption systems that it had not managed to undermine. The NSA therefore had systematic access to the private files of most Internet users, including their private bank and medical records.[137]

Indeed, in leaked internal documents the NSA boasted of its Digital Network Intelligence, including a system called XKeyscore, the NSA's "widest reaching" system.[138] XKeyscore, one document claimed, covers "nearly everything a typical user does on the [I]nternet, including the content of emails, websites visited and searches," metadata, and even social media such as Facebook chats or private messages.[139] What is more, XKeyscore, the documents state, can give the NSA (or its contractors) access to both stored and real time data.[140]

The evidence of compromise of some widely-used standards is so compelling that the National Institute of Standards and Technology (NIST), the U.S. government's standards agency charged with recommending secure protocols for encryption, has recommended against using its own standard for "Dual Elliptic Curve Deterministic Random Bit Generation," and re-opened the period for public comment on it and two other standards that may have been compromised.[141] The same vulnerability compromised the default implementation of RSA, one of the most commonly used commercial encryption standards, and after the publicity the company issued an advisory to developer customers on how to work around it.[142]

In light of these revelations, it becomes harder and harder to disagree with John Gilmore, who after describing various problems with the troubled IPSEC online encryption standard recently concluded that,

> To this day, no mobile telephone standards committee has considered or adopted any end-to-end (phone-to-phone) privacy protocols. This is because the big companies involved, huge telcos, are all in bed with NSA to make

---

[136] *See* James Ball et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN, Sept. 5, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[137] *Id.*; *see also* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071 (2013).

[138] *See* Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet,"* GUARDIAN, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[139] *Id.* (internal quotation marks omitted).

[140] *Id.*

[141] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013 (2013), *available at* http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf.

[142] *See* Kim Zetter, *RSA Tells Its Developer Customers: Stop Using NSA-Linked Algorithm*, WIRED (Sept. 19, 2013, 6:46 PM), http://www.wired.com/threatlevel/2013/09/rsa-advisory-nsa-algorithm/.

> damn sure that working end-to-end encryption never becomes the default on mobile phones.[143]

Whether or not Gilmore is correct as to the intent of the various actors, there now seems little doubt that any prudent person must assume that many if not all of the most commonly used Internet communications tools—and also the most commonly used Internet security and encryption tools—have back doors or work-arounds known to the U.S. government, the UK government, and possibly other governments also.[144] It is a truism of security research that if a product has a back door, in time the means of access will either leak or be independently discovered by third parties, including criminals; this is part of the reason why the introduction of even very secret back doors is considered to severely compromise security software.[145]

At present it seems no security technology can be trusted.[146] There is even a suggestion that the NSA may have put vulnerabilities into critical security hardware, sabotaging microchip production so as to insert back doors into random number generators, using a process that is almost impossible to detect once the chips have left the factory.[147]

The natural result of these revelations is a high degree of concern all over the world. For example, reports suggested the German Government feared,

---

[143] John Gilmore, *Re: [Cryptography] Opening Discussion: Speculation on "BULLRUN,"* MAIL ARCHIVE (Sept. 6, 2013, 5:49 PM), http://www.mail-archive.com/cryptography@metzdowd.com/msg12325.html (message board posting).

[144] *Cf.* Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, GUARDIAN, Sept. 11, 2013, http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents. The article reports the sharing of raw intelligence, not the secret means by which it was gathered. Raw intelligence, however, will contain markers that make clear its origins as an email, a chat, or whatever. While this sharing does not immediately allow the receiving agency to acquire the capacity to acquire private communications, it will over time permit the receiving agency to deduce what types of Internet communications have been compromised and to focus their efforts on replicating the exploit.

[145] *See, e.g.*, The Economist, *NSA Subversion of Internet Security: Bad for the US, Good for Criminals*, GUARDIAN, Sept. 20, 2013, http://www.theguardian.com/commentisfree/2013/sep/20/nsa-subversion-internet-security-economist (noting that "the NSA's actions may have weakened overall internet security, on which billions of people rely for banking and payments, with backdoors that can be exploited by criminals, not just intelligence agencies").

[146] *See, e.g., Did the NSA Subvert the Security of IPv6?*, INFOSECURITY (Sept. 9, 2013), http://www.infosecurity-magazine.com/view/34405/did-the-nsa-subvert-the-security-of-ipv6/ ("The bottom line, however, is that the fabric of the internet can no longer be trusted.").

[147] *See* Bruce Schneier, *Surreptitiously Tampering with Computer Chips*, SCHNEIER ON SECURITY BLOG (Sept. 16, 2013, 1:25 PM), https://www.schneier.com/blog/archives/2013/09/surreptitiously.html (citing Georg T. Becker et al., *Stealthy Dopant-Level Hardware Trojans*, *in* WORKSHOP ON CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS 197 (2013), *available at* http://people.umass.edu/gbecker/BeckerChes13.pdf).

reasonably enough, that the DRM in Windows 8 might be "a Trojan Horse for the NSA."[148] The level of security malaise—one hesitates to label as "paranoia" something that might well be justified—has become so pervasive that when the Russian Guard Service ordered new typewriters, this was widely, if perhaps inaccurately, reported as a decision to switch to paper for its most sensitive information because no electronic device could henceforth be trusted.[149]

In the end it may matter less whether the current poor U.S. legal environment for PETs and other privacy protective technologies is mostly the result of a series of accidents or primarily the consequence of a careful plan supporting the surveillance interests of the NSA and other U.S. surveillance agencies. The bottom line is much the same: if the United States has any interest in giving life to its rhetoric of personal responsibility for data security[150] then U.S. law must be changed to become far more PET-friendly.

The NSA surveillance program was highly clandestine. Many of the people involved at the state and federal level in policy-making relating to personal security likely were not aware of the NSA's activities before the Snowden revelations. That was then: we are all on notice now. The question now that we are on notice is whether policy makers will act to halt programs designed to undermine encryption and other security or privacy-protective technologies. Rather than just treating PETs as an unfortunate and regretted casualty of other worthy objectives, the U.S. government has now been shown to be acting as if PETs were a menace to the needs of a security establishment that wants access to all personal communications, and all private data, all the time.

The U.S. National Institute of Standards and Technology has stepped up to the plate and is revising its compromised standards.[151] The Internet Engineering Task Force, a private international standards body, is considering new more robust Internet security standards.[152] U.S. legislators and regulators need to display a similar respect for information privacy or PETs will remain the functional equivalent of roadkill.

---

[148] John E. Dunn, *Is Windows 8 a Trojan Horse for the NSA? The German Government Thinks So*, TECHWORLD (Aug 22, 2013, 1:48 PM), http://news.techworld.com/security/3465259/is-windows-8-a-trojan-horse-for-the-nsa-the-german-government-thinks-so/. Subsequently, however, the German Government "published a statement significantly downplaying the claims . . . referring merely to worries over a potential technical loss of control." *Id.*

[149] *See* Miriam Elder, *Russian Guard Service Reverts to Typewriters After NSA Leaks*, GUARDIAN, July 11, 2013, http://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks. Later reports suggested that the use of typewriters as an information security practice was in fact long-standing, and the order was just to replace aging machines currently in use. *Kremlin's Order of Old-Fashioned Typewriters Sparks Media Frenzy*, RT (July 12, 2013, 1:05 AM), http://rt.com/news/typewriters-russia-order-surveillance-975/.

[150] *See supra* text accompanying notes 9–16.

[151] *See supra* text accompanying note 141.

[152] *See* Phillip Hallam-Baker, PRISM-Proof Security Considerations (Sept. 11, 2013) (unpublished manuscript), *available at* http://www.ietf.org/id/draft-hallambaker-prismproof-req-00.txt.